United Nations S/2017/104

Security Council

Distr.: General
2 February 2017

Original: English

Letter dated 1 February 2017 from the Permanent Representative of Ukraine to the United Nations addressed to the Secretary-General

I have the honour to transmit herewith a concept note for the open debate on the protection of critical infrastructure against terrorist attacks, to be held on 13 February 2017.

I would be grateful if the present letter and its annex could be circulated as a document of the Security Council.

(*Signed*) Volodymyr **Yelchenko**
Ambassador
Permanent Representative

17-01674 (E) 060217

Please recycle

Annex to the letter dated 1 February 2017 from the Permanent Representative of Ukraine to the United Nations addressed to the Secretary-General

Concept note for the open debate of the Security Council on the protection of critical infrastructure against terrorist attacks

I. Introduction

Ukraine will hold an open debate of the Security Council on the protection of critical infrastructure against terrorist attacks in connection with the item entitled "Threats to international peace and security caused by terrorist acts".

The debate will take into account the results of the Arria-formula meeting of the Security Council on counter-terrorism, organized by the delegation of Ukraine on 21 November 2016, which attested to an urgent need for Member States to maintain a high level of protection of critical infrastructures and to consolidate international efforts to increase resilience against terrorist threats, so as to prevent the loss of human life and the disruption in delivery of critical services.

II. Background

The terrorist threat has recently been growing, with Al-Qaida, Islamic State in Iraq and the Levant (ISIL), Boko Haram, Al-Shabaab, al-Nusra and the like proliferating at a fast pace in many regions of the world.

Objects of critical infrastructure have long been attractive targets for terrorist groups. Therefore, they have to be protected against a growing number of diverse threats, both physical and cyber.

Banking and finance; telecommunications; emergency services; air, maritime and rail transportation; and energy and water supply are all essential elements of modern life, along with proper functioning of governmental structures.

Attacks against such objects can result in civilian casualties, lead to damage and loss of property on a large scale, disrupt proper functioning of public services, and create chaos in societies. They may also cause widespread environmental damage, as well as significantly undermine national defence capabilities.

The advancement of science and technologies has made the objects of critical infrastructure tightly interlinked. Such interdependency therefore makes them more vulnerable to any disruptions of so-called single points of failure. Attacks against critical infrastructure dependent on information and communications technologies can be a threat multiplier with a powerful destabilizing effect.

Moreover, the environmental consequences of attacks on certain critical infrastructure could impact both a host State and neighbouring States. In this case, enhanced cooperation of relevant state authorities is of great importance.

Since in most cases, objects of critical infrastructure constitute commercial property, state authorities have to establish close cooperation with the private sector.

This requires elaboration of certain emergency preparedness standards with which the private sector would comply, so as to ensure preparedness for preventing or, if need arises, countering terrorist threats, as well as managing the consequences of possible disasters.

For that purpose, the element of protection of critical infrastructure should be properly reflected in global and national terrorism prevention programmes.

Analysis of international experience in this field points to the need for addressing a number of issues, among which are coordination and cooperation of public authorities and exchange of information on existing threats and possible vulnerabilities (arising, for example, from inadequate controls at the borders and lack of a holistic security approach, of technology and of dedicated security forces); organization of public-private security partnerships; and application of a risk-assessment approach to preventing and countering threats to critical infrastructure.

Striking examples of incidents that demonstrate such a need to improve the system of protection of critical infrastructure and strengthen international cooperation in this area in particular include the recent terrorist attacks in Belgium (at the Brussels airport on 22 March 2016), Turkey (on the government buildings in Ankara in February and March 2016 and bombings at the Istanbul international airport in June 2016) and Iraq (on a chemical plant near the city of Taj on 11 May 2016).

III. Objective

Member States are encouraged to explore ways to assess vulnerabilities, interdependencies and capabilities of, as well as the cascading effects of the impacts of terrorist attacks on, their critical infrastructure. They are also invited to consider possible preventive measures while developing national strategies and policies.

IV. Questions for consideration

- What tools do States have in place to improve the safety and security of particularly vulnerable targets, such as infrastructure facilities and public places, as well as the response to terrorist attacks perpetrated against them?
- What methods have to be promoted by States to improve responsiveness and resilience to terrorist attacks against critical infrastructure, in particular taking into account recent advances in science and technologies, in particular information and communications technologies?
- How can States strengthen the capacity of both the public and private sectors and increase public-private partnerships in order to prevent and react in an efficient manner to potential risks and threats to critical infrastructure?
- What mechanisms or platforms can be established or utilized to facilitate the development and sharing of best practices on the protection of critical infrastructure of importance to States and regions, or of international significance?

- How can the United Nations, the specialized agencies and other international and regional organizations contribute to further enhancing the effectiveness of the overall efforts to counter terrorist attacks against critical infrastructure at national, regional and international levels, in particular as regards the implementation of the United Nations Global Counter-Terrorism Strategy and other related instruments?

V. Outcome

The Security Council may wish to consider adopting a resolution aimed at mobilizing international efforts to prevent and respond to terrorist attacks against critical infrastructure through enhancing national capabilities and resilience in the face of such threats and promoting inter-State cooperation in this field.

VI. Format and briefers

The open debate will be held on 13 February 2017 at 10 a.m. in the Security Council Chamber.

The following speakers will brief the Security Council: Maria Luiza Ribeiro Viotti, Chef de Cabinet of the Secretary-General; Hamid Ali Rao, Deputy Director General of the Organization for the Prohibition of Chemical Weapons; Chris Trelawny, Special Adviser on Maritime Security and Facilitation to the Secretary-General of the International Maritime Organization; Olli Heinonen, Senior Adviser on Science and Non-proliferation at the Foundation for Defense of Democracies and former Deputy Director General of the International Atomic Energy Agency; and representatives of the private sector (to be confirmed).

The format of this open debate will follow the relevant established practice of the Security Council.

It is expected that, under rules 37 and 39 of the provisional rules of procedure of the Security Council, concerned Member States and relevant international, regional and subregional organizations and initiatives will participate in the open debate.

In accordance with paragraph 29 of the note by the President of the Security Council (S/2010/507), all participants, both members and non-members of the Council, are encouraged to deliver their statements in five minutes or less. Speakers who wish to do so may circulate, if necessary, the text of a more detailed statement to Council members and participants, without making oral statements that exceed five minutes.

17-01674